CLAIMS

We Claim:

1. A method of administering access and security on a network having a plurality of computers, comprising:

installing a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network;

one-way encrypting a password entered by a user when the user logs into a computer of the plurality of computers on the network;

checking for a match between the user identification and one-way encrypted password entered by the user and the plurality of user identifications and one-way encrypted passwords stored in the one-way encrypted password file;

enabling access to data and software contained on the computer and the network permitted by the associated privileges for the user when a match is found on the one-way encrypted password file; and

filtering and displaying messages to the user permitted by the associated privileges when a match is found on the one-way encrypted password file.

2. The method recited in claim 1, wherein the associated privileges contained in the one-way encrypted password file indicate the security level and access privileges of the user identification for access to software, data and messages contained in the computer, the network, and transmitted over the network.

3. The method recited in claim 1, wherein when one or more attempts of the user entering a user identification and one-way encrypted password have failed to match the plurality of user identifications and one-way encrypted passwords contained in the one-way encrypted password file, the method further comprising:

transmitting to a systems administrator or security officer by the computer a notification of the failure to provide a one way encrypted user identification and password that matches a user identification and one-way encrypted password stored on the one-way encrypted password file.

4. The method recited in claim 3, further comprising:

locking, upon request by the systems administrator or security officer, the computer being accessed by the user having at least one failed attempt at entering a user identification and one-way encrypted password so as to permit only access to a login screen by the user.

5. The method recited in claim 3, further comprising:

spoofing, upon request by the systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

6. The method recited in claim 3, further comprising:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system.

7. The method recited in claim 6, further comprising:

deleting, upon request by the systems administrator or security officer, a plurality of files stored in the computer system.

8. The method recited in claim 1, further comprising:

displaying to a screen on the computer system a request for re-authentication at the direction of a system administrator or security officer.

9. The method recited in claim 8, wherein the request for re-authentication comprises:

displaying a login screen having a position for entry of the user identification and password.

10. The method recited in claim 9, wherein the user identification is a role or title indicative of a level of authority of the user.

11. The method recited in claim 9, further comprising:

accessing a master password file on a computer system accessible by the systems administrator or security officer;

one-way encrypting the password; and

searching the master password file for a match of the user identification and one-way encrypted password.

12. The method recited in claim 11, further comprising:

disabling the computer system, or spoofing the user, or locking the computer system when a match is not found for the user identification and one-way encrypted password in the master password file.

13. The method recited in claim 11, wherein after the user has entered the user identification and one-way encrypted password and the user identification and one-way password has matched that found in the one-way encrypted password file, further comprising:

entering a new password by the user;

re-authenticating the user identification and one-way password stored on the master password file;

one-way encrypting the new password; and

replacing the user identification and password with the one-way encrypted user identification and the new one-way encrypted password in the master password file.

14. The method recited in claim 13, further comprising:

attaching the master password file to a message;

encrypting the message using a private key and passphrase available only to the systems administrator or security officer; and

transmitting the message to the plurality of computers.

15. The method recited in claim 14, further comprising:

decrypting the message using a public key corresponding to the private key;

reporting to the system administrator or security officer a failure to decrypt the message; and

replacing the one-way encrypted password file with the decrypted master password file.

16. The method recited in claim 1, further comprising:

detecting an anomalous event in a computer of the plurality of computers; and

reporting the anomalous event to a system administrator or security officer.

17. The method recited in claim 16, wherein the anomalous event comprises:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

18. The method recited in claim 16, further comprising:

deleting a plurality of files on the computer and disabling the computer in response to an anomalous event when requested by the system administrator or security officer or when an immediate shutdown in requested by the user.

19. The method recited in claim 17, further comprising:

disabling the computer system, or spoofing the user, or locking the computer system when an anomalous event occurs.

20. A system to administer access and security on a network having a plurality of computers, comprising:

a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network;

a user login module to receive a user identification or role and password from a user and login the user when a match is found in the one-way encrypted password file; and

a channel monitoring and filtering module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

21. The system recited in claim 20, further comprising:

a password management module to update and insure that all the computers in the network contain the same one-way encrypted password file.

22. The system recited in claim 20, further comprising:

a remote auditing module to monitor and process anomalous events which may occur on the computer.

23. The system recited in claim 22, wherein the anomalous events comprise:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

24. The system recited in claim 20, further comprises:

a remote control module to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event.

25. The system recited in claim 24, wherein the appropriate action comprises:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and

deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer.

26. The system recited in claim 24, wherein the appropriate action comprises:

spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

27. The system recited in claim 24, wherein the appropriate action comprises:

locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password.

28. The system recited in claim 20, further comprising:

an authentication module to re-authenticate the user after the user login module has found a match in the one-way encrypted password contained in the computer by

checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer.

29. The system recited in claim 21, wherein the password management module attaches a master password file containing a complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and passphrase for the system administrator or security officer and broadcasts the message to all users.

30. The system recited in claim 29, wherein the password management module decrypts the message using a public key associated with the private key, replaces the one-way encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful.

31. A computer program executable by a computer and embedded in a computer readable medium to administer access and security on a network having a plurality of computers, comprising:

a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and

associated privileges for each authorized user allowed access to the plurality of computers and the network;

a user login code segment to receive a user identification or role and password from a user and login the user when a match is found in the one-way encrypted password file; and

a channel monitoring and filtering code segment to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

32. The computer program recited in claim 31, further comprising:

a password management code segment to update and insure that all the computers in the network contain the same one-way encrypted password file.

33. The computer program recited in claim 31, further comprising:

a remote auditing code segment to monitor and process anomalous events which may occur on the computer.

34. The computer program recited in claim 33, wherein the anomalous events comprise:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

35. The computer program recited in claim 31, a remote control code segment to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event.

36. The computer program recited in claim 35, wherein the appropriate action comprises:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and

deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer.

37. The computer program recited in claim 35, wherein the appropriate action comprises:

spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

38. The computer program recited in claim 35, wherein the appropriate action comprises:

locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password.

39. The computer program recited in claim 31, further comprising:

an authentication code segment to re-authenticate the user after the user login code segment has found a match in the one-way encrypted password contain in the computer by checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer.

40. The computer program recited in claim 32, wherein the password management code segment attaches a master password file containing a complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and passphrase for the system administrator or security officer and broadcasts the message to all users.

41. The computer program recited in claim 40, wherein the password management code segment decrypts the message using a public key associated with the private key, replaces the one-way encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful.